PCT/EP+ 99/06187

BUNDESREPUBLIK DEUTSCHLAND

EP99/6187

EJU

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 23 NOV 1999
WIPO PCT

Bescheinigung

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zum Generieren von digitalen Wasserzeichen für elektronische Dokumente"

am 9. Oktober 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 9/32 der Internationalen Patentklassifikation erhalten.

München, den 27. September 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiebinger

Aktenzeichen: 198 47 943.3

A 9161
06.98
11/98

P 97124

Verfahren zum Generieren von digitalen Wasserzeichen für elektronische Dokumente

(2) Patentansprüche

1. Verfahren zum Generieren von digitalen Wasserzeichen für elektronische Dokumente, bei dem vom Eigentümer eines Dokuments ein Identitätsnachweis id im Dokument derart versteckt wird, daß dieser nur mit Hilfe eines geheimen Schlüssels sichtbar gemacht werden kann, d a d u r c h g e k e n n z e i c h n e t, daß
das digitale Wasserzeichen vor dem Verstecken neben dem Identitätsnachweis id mit dem Hashwert h(m) des Dokuments versehen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das digitale Wasserzeichen vor dem Verstecken neben dem Identitätsnachweis id mit einem authentischen Zeitstempel versehen wird, der neben dem Zeitwert t mindestens auch den Hashwert h(m) des Dokuments enthält.

P 97124

Verfahren zum Generieren von digitalen Wasserzeichen für elektronische Dokumente

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren der im Oberbegriff des Patentanspruchs 1 näher bezeichneten Art, das im Postscript, JPEG, MPEG-1 beschrieben ist.

Dokumente, die in elektronischer Form vorliegen, sind ohne Qualitätsverlust beliebig oft kopierbar. Es müssen daher möglichst zuverlässige Verfahren eingesetzt werden, die eine unkontrollierte Verteilung solcher Dokumente verhindern, um die Rechte des geistigen Eigentümers zu schützen.

Durch das schnelle Wachstum des Internets und die dadurch entstandene Möglichkeit, Dokumente digital zu verbreiten, entsteht ein steigender Bedarf zum Schutz vor illegaler Verbreitung von Dokumenten und damit zum Schutz eines Copyrightinhabers vor Raubkopien.

Zu diesem Zweck arbeiten große Firmen, wie IBM, NEC und Microsoft, aber auch kleinere Firmen, wie Digimarc (siehe Funkschau 17/97; S. 21) und Forschungsinstitute, wie die Fraunhofergesellschaft IGD und die GMD Darmstadt daran, sogenannte digitale Wasserzeichen in Dokumente einzubetten. Bei Verfahren auf dieser Grundlage wird eine Information, die den Copyrightinhaber identifiziert, unsichtbar in die zu schützenden Dokumente eingebracht. Es wird im Dokument so versteckt, daß kein Außenstehender es entdecken kann.. Nur der Eigentümer selbst kann mit Hilfe seines geheimen Schlüssels das Wasserzeichen sichtbar machen und so, z. B. im Falle eines Rechtsstreits, beweisen, daß er tatsächlich der

...

Eigentümer ist. Die Art des eingebrachten digitalen Wasserzeichens kann unterschiedlich sein und hängt dabei vom jeweiligen Typ des Dokuments ab (z. B. Postscript, JPEG, MPEG-1).

Digitale Wasserzeichen erlauben es dem Copyrightinhaber, sein geistiges Eigentum an einem illegal verteilten Dokument nachzuweisen. Digitale Wasserzeichen erlauben es jedoch nicht, den Verursacher der illegalen Verteilung zu ermitteln und ihm die illegale Verteilung nachzuweisen, weil es, im Gegensatz zum elektronischen Fingerabdruck, keine Hinweise auf einen berechtigten Empfänger einer Kopie des Dokuments enthält. Ein solcher Empfänger, der bei einer Weiterverteilung selbst als Urheber auftreten will, kann das Dokument ebenfalls mit seinem digitalen Wasserzeichen versehen. Das kann zu der paradoxen Situation führen, daß im Falle eines Rechtsstreits beide Kontrahenten ihr Wasserzeichen im strittigen Dokument nachweisen können und sich gegenseitig der unerlaubten Kopie beschuldigen.

Das Gericht kann in einem solchen Fall nur dann eine korrekte Entscheidung fällen, wenn der wahre Urheber noch ein Dokument ohne beide Wasserzeichen oder nur mit seinem Wasserzeichen, ohne das des Kontrahenten, nachweisen kann. Das kann jedoch, besonders bei sehr umfangreichen Dokumenten, die nur in einer mit digitalem Wasserzeichen versehenen Kopie auf einem öffentlich zugänglichen Server liegt, nicht möglich sein.

~~Die Aufgabe der Erfindung ist es, dem wahren Urheber, auch in~~ solch schwierigen Fällen, den Nachweis seines geistigen Eigentums unstrittig zu ermöglichen.
Mit dem im Kennzeichen des Patentanspruchs 1 angegebenen Verfahren wird das ermöglicht, weil damit das digitale Wasserzeichen nicht nur von der Identität des Eigentümers, sondern auch vom Dokument selbst abhängig wird.

Mit dem Kennzeichen des Patentanspruchs 2 wird dieses Verfahren so weitergebildet, daß es noch sicherer gegen Angriffe Dritter gestaltet wird.

Anhand nachfolgender Ausführungsbeispiele wird die Erfindung näher erklärt:

Entsprechend des Grundgedankens ist das Wasserzeichen nun nicht mehr allein von der Identität id des Eigentümers, sondern zusätzlich vom Dokument m abhängig. Dazu wird ein Hashwert h(m) des Dokuments m erzeugt und das Wasserzeichen (id, h(m)) im Dokument versteckt, und zwar so, daß nach Entfernung des Wasserzeichens das Dokument m in seinem ursprünglichen Zustand wieder hergestellt werden kann.

Würde nun ein Angreifer die gleiche Strategie, wie oben zitiert, verfolgen, so würde folgendes passieren:

- Der wahre Urheber A legt das Dokument m´ auf einem Server ab, das man erhält, wenn man in m das Wasserzeichen (a,h(m)) einfügt.
- Ein Angreifer B dieses Dokument m´´, indem er in m´ zusätzlich das Wasserzeichen (b,h(m´)) einfügt.
- Das Gericht kann nun ein Verfahren dadurch entscheiden, indem es die beiden Kontrahenten auffordert, ihre Wasserzeichen (a) offenzulegen und dann (b) aus dem Dokument zu entfernen. Dann kann das Gericht aus dem wasserzeichenfreien Dokument m den Hashwert h(m) berechnen und überprüfen, in welchem der beiden Wasserzeichen dieser Wert enthalten ist.
- Alternativ bzw. zusätzlich könnte das Gericht auch beide Kontrahenten dazu auffordern, jeweils ihr Wasserzeichen zu entfernen, und dann aus den beiden verschiedenen Dokumenten m´ und m* die Hashwerte berechnen und prüfen, in welchem Wasserzeichen diese Hashwerte enthalten sind.

...

Die erwähnte Weiterbildung des Verfahrens beruht darauf, daß in das Wasserzeichen ein authentischer Zeitstempel mit eingeht. Ein solcher authentischer Zeitstempel ist dabei ein Zeitwert t zusammen mit Zusatzinformation x, der von einer unabhängigen Institution mit einer digitalen Unterschrift, etwa in der Form sig(t,x), versehen wurde.

Das in das Dokument einzubringende Wasserzeichen besteht in diesem Fall aus einem authentischen Zeitstempel, bei dem die Zusatzinformation mindestens den Hashwert h(m) des Dokuments m enthält, und der Identität des Eigentümers, z. B. in den Formen: (a,sig(t,h(m))) oder sig(t,(a,h(m))).

P 97124

1. Verfahren zum Generieren von digitalen Wasserzeichen für elektronische Dokumente

2. Zusammenfassung

2.1. Die Erfindung bezieht sich auf den Nachweis der wahren Urheberschaft anhand von digitalen Wasserzeichen.

2.2. Zur Verbesserung der Möglichkeiten in strittigen Fällen wird das digitale Wasserzeichen vor dem Verstecken neben dem Identitätsnachweis id mit dem Hashwert h(m) des Dokuments versehen und kann weiterhin noch mit einem Zeitwert t versehen werden.

2.3. Das Verfahren eignet sich zum Nachweis der wahren Urheberschaft von Dokumenten, die dem Copyrightschutz unterliegen.

This Page Blank (uspto)